Kenya's Cyber Diplomacy at the UN

POLICY BRIEF

KICTANet
The Power of Communities
www.kictanet.or.ke

GLOBAL PARTNERS DIGITAL

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.or.ke
Web: www.kictanet.or.ke
Twitter: @kictanet

Programme:
Shaping Global Cybernorms

Support:
The publication of this policy brief has been made possible through support by the Global Partners Digital (GPD

Author:
Jonas K. E. Pauly

Editors:
Victor Kapiyo and Grace Githaiga

Design & Layout:
Stanley K. Murage (stanmuus@gmail.com, Cell:+254 720316292)

Photo (Title):
Isometric data security backgroundon from Freepik, https://www.freepik.com/

Location:
Nairobi

Year of publication:
Policy Brief, July 2021

1. Introduction

Due to the transnational and borderless nature of the internet, cybercrime has become a commonplace.

Therefore, the struggle for cybersecurity must be a collective and international undertaking.

Indeed, stakeholders such the academia, businesses, civil society, governments, media and the technical community are actively working on and implementing various initiatives to enhance cybersecurity.

While many of these initiatives develop within national, regional, international frameworks, the United Nations (UN) stands out as the key global arena in which international norms governing cyberspace are negotiated.

It is also at the UN-level where the different understandings of cybersecurity clash, and where there has been some dynamism over the past three years.

This policy brief looks at the relevant cyber diplomacy developments within the UN with a focus on Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, which concluded its work in March 2021.

It provides an introduction to the power dynamics that sets the stage and deciphers Kenya's positioning within the field of nations.

Against the backdrop laid out in the following section, Kenya should be aware that capacity building, including the focus of Kenya's cyber diplomacy, can never be neutral, and that the government should make sure a human-centric and rights-based approach is pursued.

This paper draws primarily from the input provided by Kenyan representatives during the formal sessions of the OEWG between September 2019 and March 2021.

It is also complemented by relevant UN press coverage, secondary and grey literature.

The following section provides a brief introduction to the UN Group of Governmental Experts (GGE) and the OEWG, which are the main UN bodies working on the issue of cybersecurity.

Subsequently, the paper explains the main issues of contention between the United States-led camp of States and the other led by Russia and China.

As the key sponsors of relevant resolutions and bodies, their competition sets the stage on which states like Kenya find themselves. This provides the backdrop for the analysis of Nairobi's position during the OEWG and the UN in general. The paper concludes with policy recommendations for Kenya's cyber-diplomacy.

2. GGE and OEWG: 23 Years of Cyber Diplomacy

To make sense of Kenya's position in the OEWG, the body needs to be understood in the context of the history of UN discussions on cybersecurity.

In November 1998, the Russian Federation was the first to bring cybersecurity discussions to the attention of the UN in the Resolution A/53/576 on "Developments in the field of information and telecommunications in the context of international security."

In December 2003, the Russian Federation sponsored Resolution A/RES/58/32 for the establishment of the first UN Group of Governmental Experts (UN GGE). The initiative was received positively, and the resolution was adopted without a vote.

In it, theGeneral Assembly urged States to consider "existing and potential threats in the field of information security, as well as possible

measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information."

Unlike the General Assembly, membership to the GGE is limited. Of those States that have declared their interest in joining the forum, the Office of the High Representative for Disarmament Affairs and the Secretary-General select countries to the GGE membership, based on geographical and political allocation. The list of participating countries is provided in table 1. The decision making procedure in this forum is based on consensus.

2004-2005	2009-2010	2012-2013	2014-2015	2016-2017	2019-2021
A/RES/58/32	A/RES/60/45	A/RES/66/24	A/RES/68/243	A/RES/70/237	A/RES/73/266
Belarus	Belarus	Argentina	Belarus	Australia	Australia
Brazil	Brazil	Australia	Brazil	Botswana	Brazil
China	China	Belarus	Canada	Brazil	China
France	Estonia	Canada	China	Canada	Estonia
Germany	France	China	Colombia	China	France
India	Germany	Egypt	Egypt	Cuba	Germany
Jordan	India	Estonia	Estonia	Egypt	India
Malaysia	Israel	France	France	Estonia	Indonesia
Mali	Italy	Germany	Germany	Finland	Japan
Mexico	Qatar	India	Ghana	France	Jordan
Russia	Russia	Indonesia	Israel	Germany	Kazakhstan
South Africa	South Africa	Japan	Japan	India	Kenya
UK	UK	Russia	Kenya	Indonesia	Mauritius
USA	USA	UK	Malaysia	Japan	Mexico
		USA	Mexico	Kazakhstan	Morocco
			Pakistan	Kenya	Netherlands
			Russia	Mexico	Norway
			Spain	Netherlands	Romania
			UK	Russia	Russia
			USA	Senegal	Singapore
				Serbia	South Africa
				South Korea	Switzerland
				Switzerland	UK
				UK	USA
				USA	Uruguay

Table 1: List of states participating in the GGE.

While the first GGE was not able to agree on its findings, consensus reports were reached in 2010, 2013 and 2015. In 2010, the GGE focused on what should be considered a threat in cyberspace.

Three years later, the **2012-2013 GGE** achieved a milestone, in recognizing the general applicability of International Law, especially the Charter of the United Nations, to cyberspace (Broeders & Cristiano 2020, 1).

In 2015, the GGE reached consensus on eleven recommendations "for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment".

Despite the three preceding **GGEs** managing to find consensus, the process collapsed in 2017. A closer look at the applicability of International Humanitarian Law (IHL), reveals that the rules made to govern states in conflict, was a contentious issue.

While the United States and its supporters argued in favour of IHL applicability, the governmental experts from Russia, Cuba and China expressed their opposition. In addition, the 2016-2017 process witnessed increased geopolitical tensions between great powers (Ruhl et al. 2020, 5-6).

Despite this setback, the USA sponsored Resolution **A/RES/73/266** to establish a new **GGE (2019-2021) in 2018**. This time, twelve States objected to it, 16 abstained and 27 avoided to vote. In total, 55 (28.5 per cent) of the 193 Member States did not support the establishment of a new **GGE.**

During the same General Assembly session, the Russian delegation, together with 30 other States sponsored a partially competing Resolution **A/RES/73/27** establishing the "Open-ended working group on developments in the field of information and telecommunications in the context of international security".

This group would be open to all UN Member States and civil society organisations registered at the UN Economic and Social Council **(ECOSOC)**.

The OEWG aimed to be a "more democratic, inclusive and transparent" process, and was tasked to:

- Further develop the rules, norms and principles of responsible state behavior of States and ways for their implementation;
- If necessary, introduce changes to them or elaborate additional rules of behaviour;
- Study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the UN;
- Continue to study, with a view to promoting common understandings,existing and potential threats in the sphere of information security and possible cooperative measures to address them;
- [To continue to study] how international law applies to the use of information and communication technologies by States;
- [To continue to study] confidence-building measures and capacity-building;
- To submit a report on the results of the study to the General Assembly.

This resolution was even more controversial, having been opposed by 46 States, with 14 abstentions and 14 States decided not to vote. Only 61.7 per cent of all eligible States voted in its favour.

1. Algeria, Angola, Azerbaijan, Belarus, Bolivia, Burundi, Cambodia, China, Cuba, North Korea, DR Congo, Eritrea, Iran, Kazakhstan, Laos, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Pakistan, Russia, Samoa, Sierra Leone, Suriname, Syria, Tajikistan, Turkmenistan, Uzbekistan, Venezuela and Zimbabwe.

As figure 1 shows, the GGE and the OEWG turned out to be championed by the USA or Russia and China and their allies respectively.

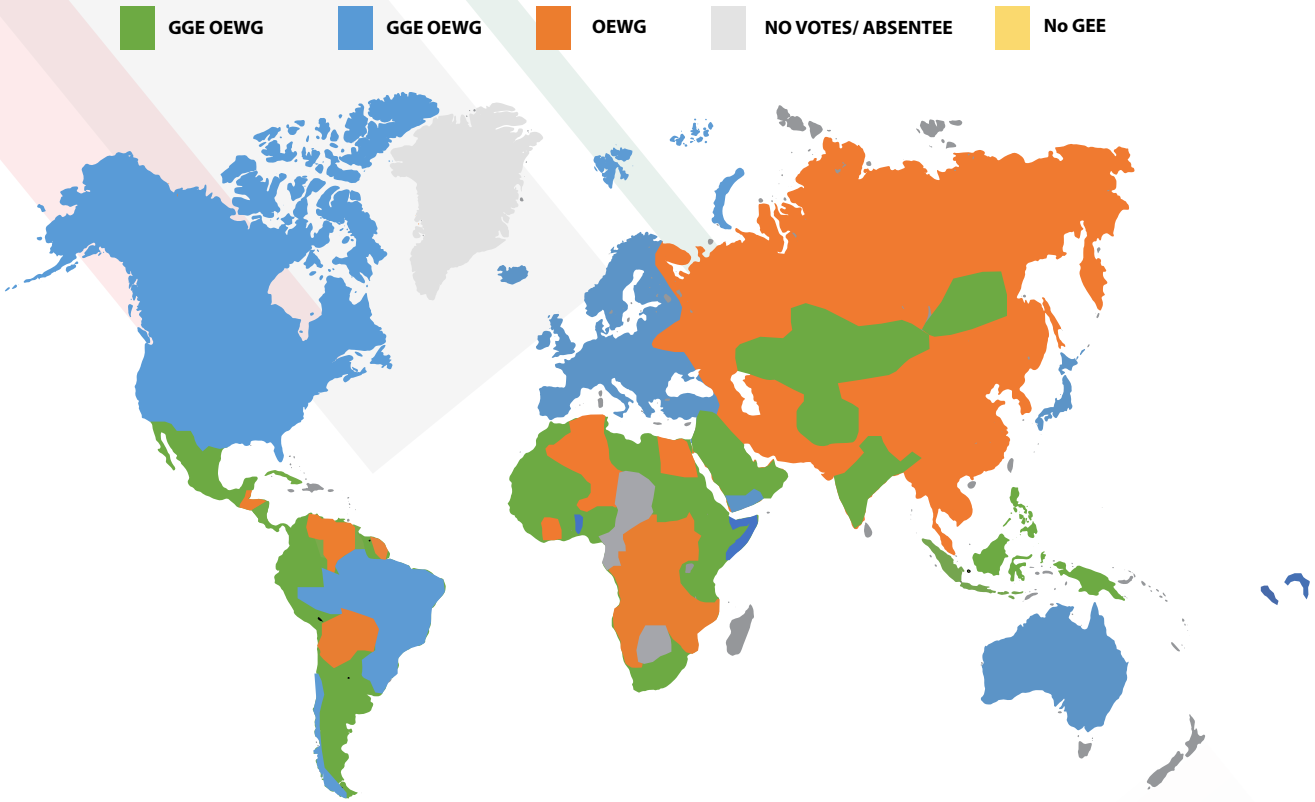

Figure 1: Voting Behaviour for GGE and OEWG.

The following section explores the substantial differences between the two blocs at the time, while the fourth section looks at Kenya's positioning in this field.

3. What are the key points of contention?

The previous section focused on the different fora which the two camps promoted.

However, the discussion is not only one of door signs, but it has a substantive foundation with two questions laying at the heart of the debate: First, what is cybersecurity about?

And, secondly, whether cyberspace is too different from the offline world that established principles of international law could (or could not) apply to it? Moreover, the two groups of States stress different rights or responsibilities of states in cyberspace.

Together with secondary literature, the statements made by the United States, China and Russia during the high-level open debate at the UN Security Council in June 2021 serve as excellent illustrations of the differing approaches (Security Council Report 2021; UN Media 2021; UN Security Council 2021).

The first question could be broken down to whether the UN should be concerned with international information security or cybersecurity.

The former term, used by the Russian Federation, is based on the idea that online content itself can be a threat to security. In authoritarian political contexts, control of online content is of utmost relevance for domestic stability.

On the contrary, the U.S.-led camp of states focuses on cybersecurity, describing primarily

the technical aspects of data "confidentiality, availability and integrity" (**Kreuzer 2018; Maurer 2020, 287; Scherman & Raymond 2019; Basu et al. 2021).**

Kreuzer (2018) describes the two kinds of risks as technical cyber security risks and content-based information security risks.

To add some nuance to this rough characterization, the Western camp of states has gradually recognized a need to regulate content in cyberspace.

The past presidential elections in the United States as well as the COVID-19 pandemic illustrated the danger of misinformation and disinformation (fake news).

Of course, such regulation is conceived in terms of individual political rights and under the rule of law. Nonetheless, respective regulatory measures by Western states provide the Russian and Chinese delegations with new points of reference to justify their positions.

The second question is, how different is cyberspace from the offline world? Maurer (2020, 289) calls this debate the validity contestation regarding existing international law. The United States highlights the similarity between the offline world and cyberspace.

Common phrases that promote this understanding are such as that made by Thomas-Greenfield (2021), the U.S. ambassador to the UN. He said, "The same rights that people have offline – including the rights of freedom of expression, association, and peaceful assembly – must also be protected online."

Their opponents, on the other side, emphasise the peerless nature of cyberspace which does allow for a simple transfer of existing international law to cyberspace. Both camps' motivations for these positions are rather clear.

While the United States championed the process of International Law formation in the period after the second world war, China now finds itself in a much more powerful situation right now. Therefore, it can hope for a much bigger say in today's negotiations.

The validity debate was partially settled in 2013 when the third GGE (2012-2013) in its report concluded that "International law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment". Since then, the key debate has been around questions of applicability.

While Western camp of states considers this matter to be of technical nature only, Russia made it quite clear that the debate was far from over, with its representative to the UN stating in June 2021 that: "although the digital sphere is not unregulated, discussions of how exactly international law can apply to it are far from over.

These questions will need to be discussed at least for another five years at the relevant UN General Assembly body, the new OEWG."

As earlier mentioned, the fifth GGE collapsed over the question whether IHL, the law governing state conduct during conflicts, applies to cyberspace.

The United States and its supporters consider it a matter of coherence that IHL, as a part of the international law body, applies to cyberspace (Agarwal 2018, 276; Ittelson 2021).

For them cyberspace is already a field of inter-state conflict given the prevalence of state-sponsored cyberattacks.

This may also be illustrated by the fact that countries are increasingly launching a fourth branch of their armed forces that focus on cyberspace. It is only a matter of time that national militaries will develop offensive military capabilities in cyberspace.

Given the already existing military relevance of cyberspace, it is only logical to pursue initiatives to regulate state conduct in cyberspace accordingly.

The Russian, Chinese and Cuban delegations, in contrast, considered this an unnecessary militarization of cyberspace. As the Russian ambassador to the UN made clear: "Of particular concern is the stance of a number of

2. Speech by the Russian Ambassador to the United Nations during the open Security Council debate on Cybersecurity on June 29, 2021.

3. Ibid.

technologically advanced states to militarize the information space by advancing the concept of so-called preventive military cyber-strikes." In this group's understanding, the U.S. assumption works as a self-fulfilling prophecy.

In contrast, the Chinese ambassador to the UN believes it is possible to "prevent cyberspace from becoming a new battlefield."
A third point of contention between the two camps lies in their diverging emphasis regarding states' rights or responsibilities. Russia and China frequently invoke the language of state sovereignty and cyber sovereignty (Agarwal 2018, 276; Creemers 2020, 12, Segal 2020).

Zhang, the Chinese ambassador to the UN speaks of the necessity "to respect the rights of all countries to independently choose their path of internet development, internet management model and to participate in the governance of cyberspace on an equal footing."

The same was reiterated by his Russian colleague stressing that Russia "stand[s] for the inviolability of state sovereignty in the digital sphere. Each country must independently determine the parameters of how they regulate their own information space and corresponding infrastructure."

This language and their joint initiative for the more inclusive OEWG allows Russia and China to present themselves as international democrats, fighting for all states' equal participation in cyberspace governance. In addition, both ambassadors laid a stronger emphasis on assisting developing countries to build up cybersecurity capabilities than their US counterparts.

On the Western side, Ambassador Thomas-Greenfield (2021) also spoke about states and their roles, but with a different perspective. She was not emphasising states' freedom to determine their national cyber policies but rather, their international obligations which are derived from the acquis on cybersecurity:

The [UN] framework [on cybersecurity] also considers how states should cooperate to mitigate the effects of significant, malicious cyber activity, imitating from a particular state's territory, including those activities undertaken by criminals. We all share this responsibility. … So let me be clear:

When a state is notified of harmful activities emanating from its own territory, it must take reasonable steps to address it… The framework UN member states have worked so hard to develop, now, provides the rules of the road. We have all committed to this framework. Now, it's time to put it into practice.

To, again, add some nuance, we must acknowledge that EU Member States started to speak about issues like data or digital sovereignty (cf. eu2020.de; Bertuzzi 2021). Yet, this refers mainly to attempts to be less dependent on US or China ICT equipment and software, and not the idea to develop something like a national, state-controlled version of the internet.

Concluding this section, one may disapprove the idea that it is again the United States, Russia and China setting up the field in which other states have to position themselves.

Yet, the past initiatives under the auspices of the UN (section 2) and the key issues of contention (section 3) illustrate that countries like Kenya have to acknowledge this development as a fact. Therefore, the following section analyses Kenya's contribution to the OEWG (2019-2021) process against this unfolded backdrop.

> ***"The same rights that people have offline – including the rights of freedom of expression, association, and peaceful assembly – must also be protected online."***

4. Speech by the Chinese Ambassador Zhang Jun to the United Nations during the open Security Council debate on Cybersecurity on June 29, 2021.
5. Ibid
6. See Note no. 2
7. This aspect of equal participation for alle states in cyber negotiations runs through the Chinese and Russian contributions during the UNSC debate.

4. Kenya's Positioning

In June 2021, the OEWG, chaired by the Swiss Ambassador Lauber, convened for three-day substantive sessions to hear States' contributions.

During the sessions, Kenyan delegates made eight contributions which inform this analysis together with the statement made by Cabinet Secretary (CS) in the Ministry of ICT and Youth Affairs, Joe Mucheru, during the Security Council open debate.

a). Commitment to the Acquis and the parallel GGE-OEWG Process

First, Kenya's contributions reveal a strong commitment to the achievements of the past GGEs and the bifurcated process of the GGE and OEWG.

It was common for the delegation to open their remarks by expressing their commitment to the consensus reports of 2013 and 2015.

Consequently, Kenya understood that the OEWG should focus on "how to operationalize already agreed-upon norms" and to raise awareness of these existing norms.

Placed in the field created by the United States, Russia and China, this position is closely aligned to the Western perspective. When initiating the OEWG in 2018, the Russian delegation tried to discredit the achievements of the GGE, saying that the "practice of some 'club agreements' should be sent into the annals of history" (UN General Assembly 2018).

The same was the case during the Russian Ambassador's speech in the UN Security Council, declaring the debate about International Law's applicability to cyberspace far from over. That the Kenyan delegation did not support this view may partially be explained by Kenya's participation in the last two GGEs.

Regarding the institutional setup of international diplomacy at the UN, the Kenyan representatives showed an almost surprising level of satisfaction.

Despite the obvious overlap of the two mandates (cf. Stauffacher 2019), the Kenyan representative understood both processes to be "mutually complementary".

Addressing the issue of regular institutional dialogue, Kenya called explicitly "upon the continuation of the GGE and OEWG framework with the already established mandates in purpose and scope."

At the same time, Kenya's statements on the issue of international law strongly questioned a straight-forward transferability of existing norms to cyberspace. The key hindrance for that, according to the speaker, is the problem of attribution.

> ***Kenya's statements on the issue of international law strongly questioned a straight-forward transferability of existing norms to cyberspace.***

8. The focus areas were 1) Existing and Potential Threats; 2) International Law; 3) Rules, Norms and Principles; 4) Confidence Building; 5) Regular Institutional Dialogue.

9. Speech by the Kenyan Delegation at the OEWG on February 11, 2020 on "Rules, Norms and Principles."
Opening Speech by the Kenyan Delegation at the OEWG on September 10, 2019.

10. Speech by the Kenyan Delegation at the OEWG on February 13, 2020 on "Regular Institutional Dialogue"

11. Speech by the Kenyan Delegation at the OEWG on February 11, 2020 on "International Law."

b). Hackers or Bloggers? Kenya's View on Cyber threats

"Existing and potential threats" was itself an agenda item of the OEWG. Tellingly, the Kenyan delegation opened its speech by reminding States that "some countries have already developed … capabilities" for the offensive use of ICTs.

The representative recognised the threat cyber weapons posed, allowing for a new kind of warfare. Acknowledging the imminence of this scenario and the already existing military potential of cyberspace, the speaker hinted at the relevance of IHL.

This might be well received in Washington, whereas Moscow and Beijing consider the militarization of cyberspace to depend on the applicability of IHL.

In general, the threats described by Kenya during the OEWG sessions were mainly technical cyber security risks, such as breaches in confidentiality and privacy, malware and denial of service attacks.

At the Security Council level, however, two of the threats described by CS Mucheru in the Security Council high-level debate are rather content-based information security risks that bear greater potential to be abused as pretences to repress political opponents, namely "ICT and violent extremism" and "ICT and social media."

Thirdly, the Kenyan delegation used the OEWG to promote the perspective of developing countries, stressing that "the digital divide is itself a threat."

CS Mucheru used the occasion of the Security Council debate to highlight that cybercrime was increasingly focused on developing countries. Lacking the capability to detect and respond to cyberattacks, some states had a greater probability to end up as proxies or casualties of cyberconflicts.

While neither the United States nor Russia and China recognized the digital divide as a threat, it is the latter two who hinted at the relevance of capacity building for developing countries more strongly.

In general, Kenyan delegates did not invoke the language of cyber sovereignty or alike.
No cybersecurity without cyber-capacity
The focus on the digital divide as a key factor for cyberthreats hints at the key theme of all of Kenya's contributions.

Again and again, the delegation highlighted the conditional nature of cyber capacity for anything discussed in the forum. Speaking on Rules, Norms and Principles, Kenya emphasised that:
norms … require an enabling environment for the protection of critical infrastructure.

This requires articulated national policies, cyber strategies, allocation of resources, and available skilled technical professionals, many of which may not be available in some countries.

On the same note, Kenya made clear that it also considered confidence-building measures, first and foremost, an issue of capacity-building:

---

13. *"The second area relates to ICT and violent extremism. The ubiquitous programmable and data driven nature of the emerging technologies, although beneficial, has also opened a door misused by armed groups and terrorists. Those groups capitalize on the opaque control mechanisms, algorithms, 3D printing, application of cryptography and simplified user interface to recruit, plan and carry out terrorist attacks. This has enhanced radicalization and militarization" (CS Mucheru at the UNSC on June 29, 2021).*

14. *"My third focus area, Mme President, is ICT and social media. The growing impact of fake news, deep fakes, misinformation and disinformation on peace and security cannot be overstated. Recently, we have seen the impact of fake news lacking the response to covid-19 pandemic threats by promoting vaccine hesitance. The social media companies need to be held to account and made to ensure that fake news, particularly by sophisticated actors, some supported by states, is not proliferating on their platforms. Such as a regulatory effort would/will need to be built on a multilateral platform to ensure uniformity of effect" (CS Mucheru at the UNSC on June 29, 2021).*

15. *Speech by the Kenyan delegation at the OEWG on February 10, 2021 on "Existing and Potential Threats."*

16. *CS Mucheru at the UNSC on June 29, 2021*

17. *Speech by the Kenyan delegation at the OEWG on February 11, 2020 on "Rules, Norms and Principles."*

How can confidence-building measures yield intended results if some countries lack the capacity to detect, identify, investigate, defend, contain, or counter existing and potential cyber threats. Consequently, confidence-building works best between nations with sufficient capabilities and confident trust networks.

c). International Alignment

To understand how Kenya positions itself in the field unfolded by the main players of international cybersecurity diplomacy, it is important to look at the explicit references the Kenyan delegation made to other countries and bodies.

As it is clear by now, cyber-diplomacy is as much about content as it is about institutional formats.

During its opening speech, Kenya aligned itself to the Non-Aligned Movement. In this regard, Kenya's insistence on capacity building as the key for international cybersecurity spoke for a larger group of developing countries.

Speaking on the issue of women in international security and cyberspace, Kenya explicitly praised members of the Western camp, the United Kingdom, Australia, Canada, Netherlands and New Zealand, "for leading by example through the women in the international security and cyberspace fellowship."

Furthermore, when commenting on the draft report, Kenya argued for explicit reference to the Global Forum on Cyber Expertise **(GFCE).** The **GFCE** is a multistakeholder network to strengthen cyber-capacity.

The **GFCE** is an outgrowth of the series of Global Conferences on Cyberspace that was initiated in 2011 by the British government.

The **GFCE** itself was launched by the Dutch government in 2105. Kenya is one of the 94 members (consisting of states, business, and other organisations), unlike Russia or China.

Although Kenya did not serve as a co-sponsor of the proposal to establish a Programme of Action **(OEWG Joint Contribution 2021)**, these aspects can be read as a clear orientation towards the Western camp of states. Considering a wider picture at the developments under the UN umbrella, however, a blurrier image occurs.

First, one year after the authorization of the GGE (2019-2021) and OEWG (2019-2021) resolutions, Kenya voted in favour of a Russian-sponsored resolution A/RES/74/247 that allowed Russia to establish an intergovernmental committee of experts "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" (cf. Hakmeh & Vignard).

As figure 2 illustrates, this initiative was strongly rejected by the Western group of states as they expected Russia to focus on content-based information risks, providing states with additional sources of legitimacy in their censorship and repression of free speech.

18. *Speech by the Kenyan delegation at the OEWG on February 12, 2020 on "Confidence Building".*

19. *Speech on Capacity building on February 12, 2020.*

20. *Huawei joined the initiative as early as 2015.*

21. *OEWG Joint Contribution, online available at: https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf [accessed on November 21, 2021].*

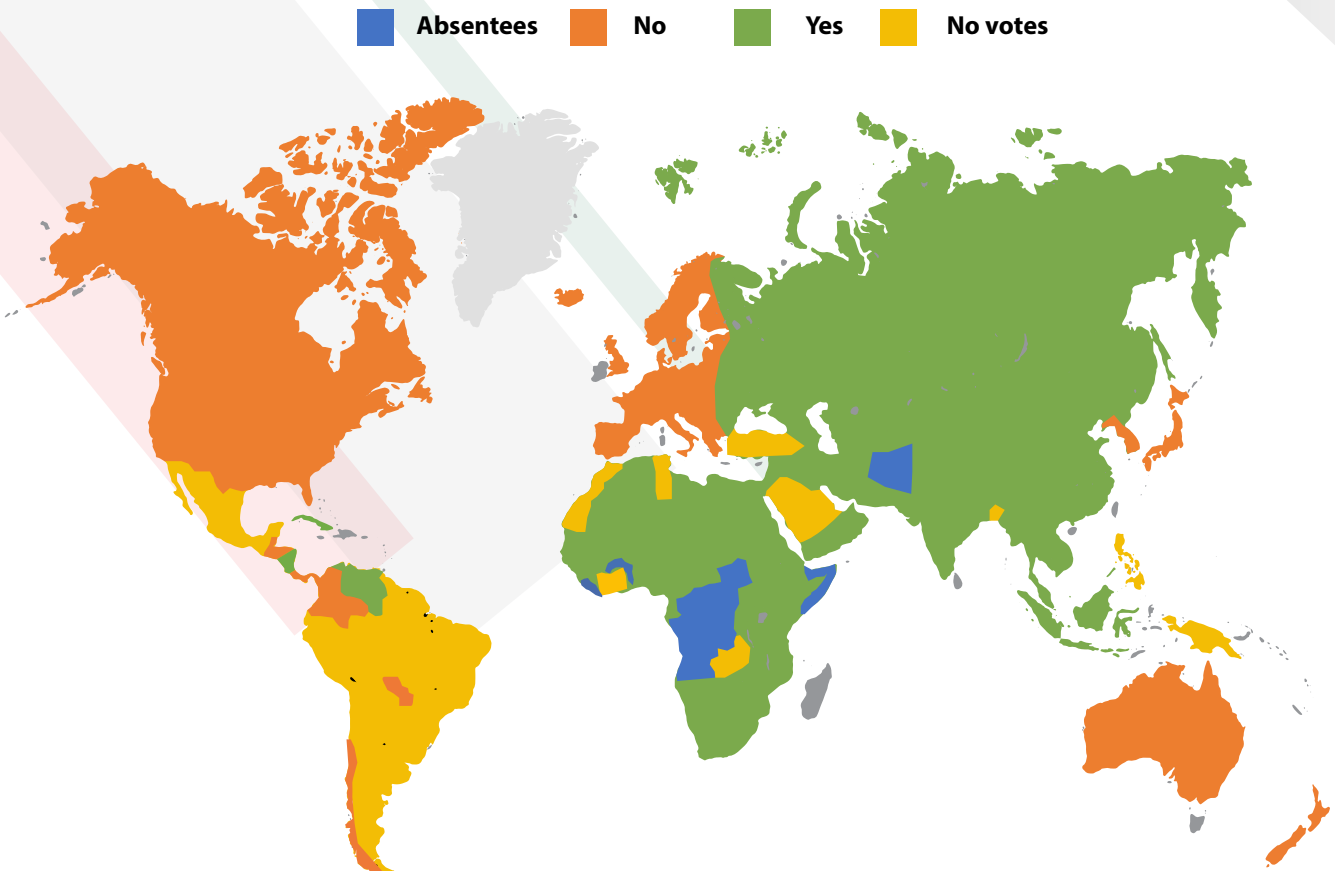

Figure 2: Voting Behaviour for A/RES/74/247.

Secondly, in May 2021, China, Mexico and Kenya organised an informal meeting on "The Impact of Emerging Technologies on International Peace and Security for Security Council members.

The meeting focused on the "the danger posed by the militarization of emerging technologies, especially if used in the context of terrorism."

While the reference to terrorism points away from interstate cyberwar, the militarization of cyberspace represents a frequent accusation of Russia and China against the United States.

In summary, Kenya showed a clear orientation towards the U.S.-led group of states in the OEWG by promoting the acquis, focusing on technical cyber security risks, avoiding the language of state sovereignty and endorsing western bodies. For Kenya's insistence on cyber capacity-building for developing countries, the Russian and Chinese delegation might be in a prime position to respond.

Furthermore, at the Security Council level, the image is less clear with Kenya stressing content-based information risks and co-organising relevant events with China.

Of course, organising a joint event does not impose the co-organizers' approach to cybersecurity in Kenya, but it lends the actor greater legitimacy to speak on the matter.

Takeaways & Recommendations

Against the canvas drawn so far, two policy recommendations are due. Both iterate and build on KICTANet's contribution to the OEWG on behalf of the Association for Progressive Communications (APC) in February 2020.

1). Kenya should recognize that capacity-building can never be neutral.

At first sight, Kenya's focus on capacity-building appears as a way to not get caught up in a great power struggle.

While China and Russia put a much stronger rhetorical emphasis on this aspect, the United States, too, recognizes the need for international cooperation to build cyber-capacity.

If given a second look, however, its seemingly neutral character disappears. Capacity is, by necessity, always a capacity to do certain things in a certain way. In the end, what cyber-capacity is depends on the understanding of cybersecurity.

States might receive training and equipment to monitor social media content, framing this as a measure against content-based information security risks; or receive training for its national computer incident response teams (CIRT), which focuses strongly on questions of data confidentiality, availability and integrity.

In the case of the Computer Misuse and Cybercrimes (Amendment) Bill 2021, the Kenyan government seems to have given in to the authoritarian temptation of instrumentalizing cybersecurity laws.

In light of this, the Kenyan government should– for the sake of its own credibility and reputation - practice transparency in how it receives and provides capacity-building measures.

2). Kenya should promote a human-centric and rights-based approach to cybersecurity

On New Year's Eve of 2020, the General Assembly adopted Resolution A/RES/75/240 for the launch of a second OEWG (2021-2025).

Almost a year later, on November 3, 2021, the First Committee of the General Assembly approved a draft resolution (document **A/C.1/76/L.13)**, co-sponsored by the United States and Russia, that acknowledged the outcomes of the past GGE and **OEWG**, and called on the new **OEWG** to be guided by these outcomes (UN Press 2021).

This reconciliation ended the bifurcated GGE-**OEWG** process in favour of the **OEWG.** The States having favoured an alternative "Programme of Action" format, expressed their willingness to continue this discussion in the **OEWG** forum (Meyer 2021, 2).

Regrettably, Paul Meyer of the ICT4Peace Foundation notes that the draft resolution, "makes no reference to the future role of civil society, the private sector and other stakeholders in the **OEWG's** work"..

Furthermore, it does not emphasise a "human-centric" approach that put's human security at the centre of international cybersecurity diplomacy.

Recalling KICTANet's contribution to the **OEWG**, it is this "human-centric and rights-based approach", that ensures that cybersecurity is not abused as a means to repress people and limit their freedoms (KICTANet 2020).

As a country that greatly benefits from its open and internationally connected ICT industry, it is in Kenya's interest to protect individual digital freedoms.

As a member to the **OEWG** as well as the intergovernmental committee of experts working on a "international convention" on cybercrimes **(A/RES/74/247),** Kenya should contribute to the adoption of a human-centric and rights-based approach and make human rights the centre of its cyber-diplomacy.

References

Agarwal, Sunil. 2018. Normative Challenges in the Cyber Domain: Limits of the UNGGE-OEWG Process. ISIL Year Book of International Humanitarian and Refugee Law, 18, 270-277.

Basu, Arindrajit; Peotranto, Irene & Lau, Justin. 2021. The UN Struggles to Make Progress on Securing Cyberspace. Carnegie Endowment for International Peace. Online available at: https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491 [accessed on November 21, 2021].

Bertuzzi, Luca. 2021. What's in sight for the EU digital sovereignty? Digital Brief. EURACTIV. Online available at: https://www.euractiv.com/section/digital/podcast/whats-in-sight-for-the-eu-digital-sovereignty/ [accessed on November 21, 2021].

Broeders, Dennis & Cristiano, Fabio. 2020. Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road. Italian Institute for International Political Studies. Online available at: https://www.ispionline.it/en/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417 [accessed on November 21, 2021].

Creemers, Rogier. 2020. China's Approach to Cyber Sovereignty. KAS. Online available at: https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537 [accessed on November 21, 2021].

dig.watch. n.d. UN GGE and OEWG. Geneva Internet. Online available at: https://dig.watch/processes/un-gge [accessed on November 21, 2021].

eu2020.de. 2020. Expanding the EU's digital sovereignty. Homepage to the German Presidency of the Council of the European Union. Online available at: https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828 [accessed on November 21, 2021].

Hakmeh, Joyce & Vignard, Kerstin. 2021. International Security, and Cybercrime: Understanding their Intersections for Better Policymaking. Geneva: UNIDIR.

Ittelson, Pavlina. 2021. What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis. Diplomacy.edu. Online available at: https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/ [accessed on November 21, 2021].

Kreuzer, Leonhard. 2018. Disentangling the cyber security debate. Völkerrechtsblog. Online available at https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/ [accessed on November 21, 2021].

Maurer, Tim. 2020. A Dose of Realism: The Contestation and Politics of Cyber Norms. Hague Journal on the Rule of Law 12: 283-305.

Mayer, Paul. 2021. Cyber Security at UNGA's First Committee 2021: An appearance of harmony. ICT4Peace Foundation. Online available at: https://ict4peace.org/wp-content/uploads/2021/11/Cyber-at-UNGA-First-Cttee-Nov-2021-1.pdf [accessed on November 21, 2021].

Ruhl, Christian; Hollis, Duncan; Hoffman, Wyatt & Maurer, Tim. 2020. Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Working Paper, Carnegie Endowment for International Peace. Online available at: https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110 [accessed on November 21, 2021].

Security Council Report. 2021. June 2021 Monthly Forecast: Cybersecurity. Online available at: https://www.securitycouncilreport.org/monthly-forecast/2021-06/cybersecurity.php [accessed on November 21, 2021].

Segal, Adam. 2020. China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In Rolland, Nadège (ed.), An Emerging China-Centric Order. Washington: National Bureau of Asian Research.

Sherman, Justin & Raymond, Mark. 2019. The U.N. passed a Russian-backed cybercrime resolution: That's not good news for Internet freedom. Washington Post. December 4. Online available at: https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/ [accessed on November 21, 2021].

Stauffacher, Daniel. 2019. UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes. ICT4Peace Foundation. Remarks to Jeju Forum May 2019. Online available at: https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf [accessed on November 21, 2021].

Thomas-Greenfield, Linda. 2021. Remarks by Ambassador Linda Thomas-Greenflied at a UN Security Council Open Debate on Cybersecurity. United States Mission to the United Nations. Online available at: https://usun.usmission.gov/remarks-by-ambassador-linda-thomas-greenfield-at-a-un-security-council-open-debate-on-cybersecurity/ [accessed on November 21, 2021].

UN General Assembly. 2018. Meetings Coverage and Press Releases. First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct. Online available at: https://www.un.org/press/en/2018/gadis3619.doc.htm [accessed on November 21, 2021].

UN General Assembly. 2021. Meetings Coverage: First Committee Approves 60 Texts, Rejects 1, with Delegates Differing over Weapons of Mass Destruction, as Action Phase Concludes. Online available at: https://www.un.org/press/en/2021/gadis3678.doc.htm [accessed on November 21, 2021].

UN Media. 2021. Cyber security – Security Council, VTC Open Debate. Online available at: https://media.un.org/asset/k1e/k1egd92tkq [accessed on November 21, 2021].

UN Security Council. 2021. Press Release: 'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats. June 29. Online available at https://www.un.org/press/en/2021/sc14563.doc.htm [accessed on November 21, 2021].

KICTANet
The Power of Communities

Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet